White Paper

Inhalt

ExtremeCloud™ IQ: Überblick über Sicherheit und Architektur der Cloud

Produktübersicht

ExtremeCloud IQ von Extreme Networks ist eine Cloud-basierte Netzwerkmanagement-Lösung, die als Software-as-a-Service (SaaS) angeboten und als Abonnement über Reseller auf der ganzen Welt verkauft wird. ExtremeCloud IQ bietet eine zentralisierte Orchestrierung der Konfiguration sowie Netzwerk-Überwachung, Reporting, Alarme und Statistiken für alle Cloud-fähigen Geräte von Extreme Networks.

Architektur-Übersicht

Geografische Verteilung

ExtremeCloud IQ wird aktuell in 17 regionalen Rechenzentren (RDC) und vier globalen Rechenzentren (GDC) eingesetzt. Ein RDC ist eine geografische Instanz der SaaS-Lösung, in der die Kundendaten gehostet werden. Der Service nutzt ausschließlich große kommerzielle Cloud-Hosting-Anbieter. Heute werden über 90 % der Lösung über Amazon AWS gehostet. Andere genutzte Anbieter sind Google GCP und Microsoft Azure.

v1.0 - Ocktober 2020

Inhalt (Forts.)

GDC

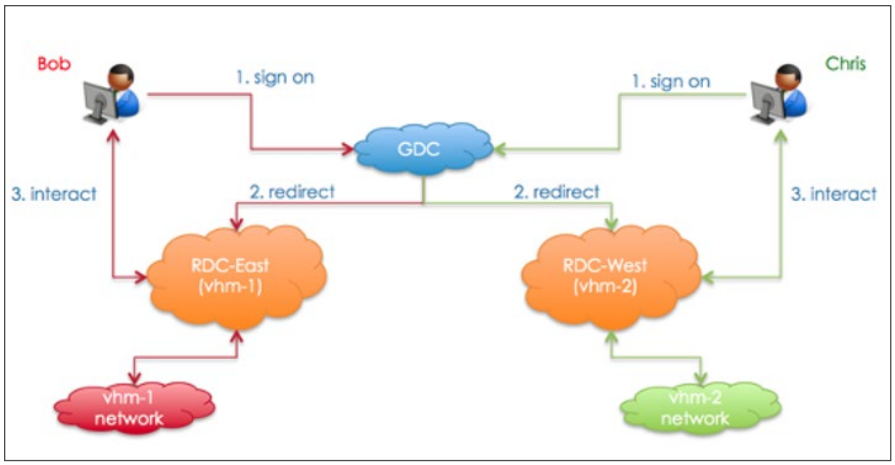
GDC	RDC Amazon (AWS)	RDC Google (GCP)	RDC Microsoft (Azure)
	90 Days Data Retention	Unlimited Data Retention	
Virginia, USA	Virginia 1, USA (VA1)	Amsterdam, Netherlands (NL-GCP)	Virginia, USA (AVA) 13 months Data Retention For Retail Customers
Oregon, USA	Virginia 2, USA (VA2)	Iowa, USA (IA-GCP)	Zürich, Switzerland (ACH) 90 days Data Retention
Dublin, Ireland	Dublin, Ireland (IE)		Toronto, Canada (ACA) Unlimited Data Retention
Frankfurt, Germany	São Paulo, Brazil (BR)		
	Stockholm, Sweden (SE)		
	Frankfurt, Germany (FR)		
	Mumbai, India (IN)		
	Tokyo, Japan (JP)		
	Sydney, Australia (AUS)		
	Manama, Bahrain (BH)		
PRIVATE RDCs			
	Oregon, USA		Virginia, USA
	Virginia, USA		
	Dublin, Ireland		
	Sydney, Australia		

NOTE: Private RDCs are NOT depicted in the above graphic

Die GDC oder Global Data Center, schaffen mit den redundanten Standorten in USA (Virginia und Oregon) und Europa (Dublin und Frankfurt) eine geografische Lastverteilung unter Berücksichtigung der jeweiligen Datenschutzregeln. Die US-Login-Informationen existieren nur auf den US-Instanzen des GDC, während EU- und andere Nationen in den beiden europäischen Instanzen gespeichert werden, um den geografischen Datenschutz zu wahren. Das GDC dient nicht nur als primärer Authentifizierungs-Mechanismus für die ExtremeCloud IQ SaaS-Plattform, sondern führt bei Bedarf auch die Umleitung von Geräten und andere globale Dienste durch. Alle Instanzen des GDC werden in Amazon AWS gehostet.

RDC

Das RDC, oder Regional Data Center, wird bei verschiedenen Cloud-Anbietern gehostet, je nach Aufbewahrungszeit und -ort der Daten. Das RDC besteht aus virtuellen Umgebungen, die als VIQ bezeichnet werden. Jeder Kunde hat sein eigenes VIQ, in dem die gesamte Interaktion mit dem Produkt stattfindet und mit dem sich die kundeneigenen Geräte verbinden. Das VIQ existiert nur auf einem einzigen RDC; das bedeutet, dass alle auf den Kunden bezogene Daten an diesem speziellen Ort gespeichert sind.



Cloud-Skalierung

ExtremeCloud IQ nutzt für die Skalierung die inhärente Flexibilität der Cloud und der Container-basierten Microservices. Je nach Bedarf können neue Server und Backend-Infrastrukturen etabliert werden, basierend auf Last, Kunden- und Partnerwachstum und als Konsequenz der Überwachung des Betriebs hinsichtlich erlernter Muster der System-Performance.

Cloud-Provider

ExtremeCloud IQ nutzt die folgenden Cloud-Provider (im Sinne der GDPR-Compliance können diese Anbieter als Sub-Prozessoren betrachtet werden):

- Amazon AWS
- Google GCP
- Microsoft Azure

Weitere Informationen zum Thema Datenschutz und Sub-Prozessoren finden Sie unter unserem Datenschutz-Link.

Container-basierte Lösung

ExtremeCloud IQ basiert als SaaS-Anwendung auf Microservices. In einer Containerarchitektur integriert, werden diese in der Umgebung unserer Cloud-Provider gehostet. Organisiert in einer 100%igen Kubernetes-Umgebung erfolgen Regelbetrieb, Überwachung und Wartung rund um die Uhr durch unsere Extreme Networks Cloud Operations Teams.

Zertifizierungen

ExtremeCloud IQ nutzt Amazon AWS, Google GCP und Microsoft Azure als Infrastruktur-Provider. Die öffentlichen Erklärungen dieser Provider zu SOC 1, 2, 3, PCI, ISO und anderen Compliance-Standards können an den folgenden Stellen eingesehen werden:

- https://aws.amazon.com/compliance/programs/
- https://cloud.google.com/security/compliance/offerings/
- https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home

Extreme Networks überprüft regelmäßig die Fähigkeiten, den Umfang und die SLAs der Anbieter. Darüberhinaus ist ExtremeCloud IQ als SaaS-Lösung nach ISO27001 zertifiziert (siehe https://cloud.kapostcontent.net/pub/d8b0c577-e7f3-457d-9669-daa3d666df61/iso-27001-certification-1)

Die Prüfung anhand dieses Regelwerkes wird regelmässig wiederholt. Zusätzlich wurden folgende Zertifizierungen erteilt:

- Cloud Security Alliance STAR Level 1
- ISO 27017 und ISO 27701
- SOC Typ 1, 2, 3

Internationale Compliance

ExtremeCloud IQ hält sich an die jeweiligen lokalen Datenrichtlinien. Die Rechenzentren in der EU führen die Datenreplikation ausschließlich innerhalb der EU-Region durch; alle Backups werden ausschließlich innerhalb der EU aufbewahrt.

ExtremeCloud IQ Sicherheit

Schutz der Datenintegrität

Daten im Transit

Der gesamte Managementverkehr von und zu ExtremeCloud IQ wird mittels CAPWAP und HTTPS umgesetzt. DTLS bzw. TLS sichern das Hoch- und Herunterladen von Datenverkehr, wie z. B. Image-Dateien der Gerätesoftware, vollständige Konfigurationen, unverschlüsselte Webportalseiten und Zertifikate. TLS 1.2 und optional TLS 1.3 werden mit Verschlüsselungsverfahren wie AES eingesetzt.

Netzwerkstatistiken und Überwachungsdaten werden ebenfalls über CAPWAP mit DTLS und/oder HTTPS-Protokoll gesendet.

Daten im Ruhezustand

Alle Daten im Ruhezustand innerhalb von ExtremeCloud IQ, die als Dateien oder in Datenbanken gespeichert werden, lagern auf verschlüsselten Speicher-Volumes. Dabei wird das AES-256-Verfahren mit Schlüsseln verwendet, die über den Cloud-Anbieter verwaltet werden. Standardmäßig werden die Schlüssel von den Anbietern alle 3 Jahre automatisch rotiert bzw. wie von den Managed Services des Cloud-Anbieters konfiguriert. Kunden können keine Verschlüsselungsschlüssel verwalten.

Protokollierung

Alle Protokolle angeschlossener Geräte können an einen zentralen Syslog-Server auf dem Campus des Kunden umgeleitet werden. Darüber hinaus ermöglicht ExtremeCloud IQ das zentrale Sammeln aller relevanten Ereignisse/Alarme/Protokolle.

Logische und physische Sicherheit

ExtremeCloud IQ Cloud Operations verwaltet proaktiv Firewall- und Netzwerk-Sicherheitsrichtlinien für die gehosteten Services. Extreme nutzt die aktuellen Best Practices der Branche in Bezug auf Sicherheits- und Zugriffsverfahren, um den logischen und physischen Zugriff und die Berechtigungen auf diese Systeme zu beschränken. Alle Zugänge zu den physischen Rechenzentren, in denen ExtremeCloud IQ gehostet wird, sind für Mitarbeiter von Extreme Networks nicht zugänglich, egal aus welchem Grund. Der gesamte Zugang zu den Einrichtungen und Grundstücken, die sich im Besitz von Extreme Networks befinden, erfolgt über einen ständig überwachten und gesperrten Zugang, einschließlich Sicherheitskameras.

Die gesamte Nutzung der Netzwerk-Services von Extreme Networks wird überwacht.

Antivirus

Alle Laptops und PCs der Mitarbeiter von Extreme Networks werden durch aktuelle Antiviren-Software geschützt.

Bösartiger und anfälliger Code

Der gesamte Code, der für die Cloud-Plattform geschrieben wird, wird täglich mit Hilfe automatisierter Testsysteme auf bösartigen Code und Sicherheitslücken überprüft. Das beinhaltet auch neu entwickelte Patches und Funktionsmodule.

Ergebnisse dieser Tests werden von der Entwicklung und von CloudOps bearbeitet. Eine Veröffentlichung findet aus Sicherheitsgründen nicht statt.

System Hardening

Alle in der Cloud-Infrastruktur verwendeten Systeme sind gemäß CIS-Benchmarks gehärtet und nutzen eine modifizierte, abgestimmte und speziell gesicherte Betriebssystemumgebung, die von Extreme Cloud Operations entwickelt wurde.

Segmentierte Umgebungen

Für Entwicklung, User Acceptance und Produktion werden separate Umgebungen betrieben.

Software-Patches von Drittanbietern

Patches von Drittanbietern werden in die Systeme von Extreme gemäß der gleichen Änderungsregeln wie die Cloud-Produktionsversionen eingespielt. Größere Versions-Upgrades der Software von Drittanbietern werden als Teil der Haupt-Entwicklungszyklen geplant, was einen länger andauernden Testzyklus und gewonnene Stabilität für dazwischenliegende Software-Releases impliziert.

Anwender-Rollen und Policies

ExtremeCloud IQ stellt administrative Optionen zur Verwaltung von Anwender-Rollen und Berechtigungsebenen für Endanwender bereit. Ein Kunde verfügt über ein einziges „Superuser“-Konto mit der Möglichkeit, zusätzliche Administratoren mit detaillierten Berechtigungen für verschiedene Funktionen zu erstellen.

Kunden, deren Konten von einem Extreme-Partner (einem Integrator oder Managed Service Provider) verwaltet werden, können den Zugriff ihres übergeordneten Partners einschränken/gewähren (z. B. um zu verhindern, dass Mitarbeiter des Partners ihr System überwachen oder konfigurieren, oder um ihnen alternativ Zugriff für die Wartung durch den Partner zu gewähren). Partner können ein Kundenkonto deaktivieren (z. B. für nicht zahlende oder gekündigte Kunden).

Account-Bereitstellung

Sobald sich ein Kunde auf https://extremecloudiq.com registriert, werden neue Accounts bereitgestellt. Von diesem, mit Admin-Rechten versehene Account können weitere Administratoren berechtigt werden.

Die Cloud Operations von Extreme haben zur Fehlerbehebung potenziell logischen Zugriff auf das System.

Passwort-Richtlinien (Zurücksetzen, Speicherung)

Es werden keine Passwörter im Klartext gespeichert. Anwender können die Option „Passwort vergessen“ auf der Anmeldeseite unter https://extremecloudiq.com nutzen, um Passwörter zurückzusetzen.

SSO, Sitzungs-Timeouts

ExtremeCloud IQ unterstützt Single Sign on mit SAML. Dieses standardbasierte Authentisierungsframework wird optional von Cloud Operations für den Kunden angefordert und konfiguriert.

Die Sitzungs wird nach einem konfigurierbaren Timeout (Standard: 30min) automatisch beendet. Alle administrativen Zugriffe werden in einem Audit-Log innerhalb der Cloud-Plattform protokolliert.

Logischer Zugriff

Cloud-Anbieter, Sub-Prozessoren und Auftragnehmer von Drittanbietern haben keinen logischen Zugriff auf die Plattform. Der gesamte Zugriff auf die Plattform durch die Mitarbeiter des Cloud-Betriebs erfolgt über eine Multi-Faktor-Authentifizierung von überprüften und autorisierten Personen nach dem „Need-to-Know“-Prinzip; der gesamte Zugriff wird außerdem von gesicherten Zugangsservern über verschlüsselte Kommunikation protokolliert und streng kontrolliert.

Cloud Operations

Die Cloud Operations-Teams (DevOps) befinden sich in den USA, Kanada, Indien und China. Der gesamte Zugriff auf die Cloud-Infrastruktur und alle von den Cloud-Services erzeugten Kundendaten erfolgt über VPN und Multi-Faktor-Authentifizierung. Die Server in den Rechenzentren in North Carolina und New Hampshire sind als gesicherte Zugangsserver für das Cloud Operations-Team und QA/Engineering für den Zugriff auf die Cloud-Infrastruktur vorgesehen. Diese Systeme werden in Übereinstimmung mit dem Business Continuity Plan von Extreme und als Teil des ISO 27001 ISMS protokolliert, gesichert und gewartet.

Software-Upgrades und QA

Extreme Networks führt regelmäßig alle Wartungsarbeiten und Updates an der Cloud-Plattform durch. Alle Updates werden vor der Freigabe getestet und einer Qualitätssicherung unterzogen; weitere Tests erfolgen nach der Freigabe in der Produktion. Die Kunden haben zu jeder Zeit die Kontrolle und entscheiden, zu welchem Zeitpunkt sie ihre Hardware (Access Points, Switches, Router) aktualisieren. Betriebssystemversionen auf diesen Geräten können variieren und sind nicht zwingend von der Cloud-Plattform vorgegeben.

Change Control-Richtlinie

Als ISO27001-zertifizierte Plattform verwendet ExtremeCloud IQ einen mehrstufigen Change-Control-Prozess (Continuous Integration/Continuous Delivery) für alle architektonischen Änderungen sowie Software-Releases und Updates. Nach der Entwicklung werden alle Updates in eine Staging-

Umgebung für die Qualitätssicherung und Produktionstests verschoben, bevor sie während der angekündigten Wartungsfenster in die Produktion überführt werden.

Datenschutz und Privatsphäre

Sensibilität der Daten

ExtremeCloud IQ bietet Zugriff auf Gerätekonfiguration, Verwaltung und Statistiken zur Netzwerküberwachung. Die gespeicherten Daten enthalten keine PII (persönlich identifizierbare Informationen) wie Sozialversicherungsnummern, Führerscheinnummern, Kontonummern oder persönliche medizinische oder Versicherungsinformationen für verbundene Geräte und Anwender. Nur sitzungsbasierte Nutzungsstatistiken und PII wie IP-Adresse, Gerätetyp, Mac-Adresse und andere Informationen, die sich auf die Verwendung eines angeschlossenen Geräts beziehen, werden gesammelt und ausgewertet. Alle PII werden mit der gleichen Übertragungs- und Speicherungs-Sicherheit behandelt wie alle Daten und sind zu jeder Zeit verschlüsselt.

Keine rohen TCP/IP-Sitzungen (Packet Capture) oder andere Daten, die verwaltete Netzkomponenten durchlaufen (z. B. Anwender A, der sich bei Server B anmeldet, um Bankdaten über verwaltete drahtlose APs, Switches und Router zu überprüfen), werden auf der ExtremeCloud IQ SaaS-Plattform übertragen, kontaktiert oder gespeichert.

Alle Kundendaten sind privat! Sie bleiben im Besitz des Kunden und können jederzeit gelöscht werden.

In der Cloud Services-Plattform verfügbare Daten und PII

Eine detaillierte Auflistung der erfassten Daten finden Sie in der angehängten Datenschutz-Matrix am Ende dieses Dokuments.

Hintergrund-Checks

Alle Mitarbeiter von Cloud Operations und andere beteiligte Mitarbeiter, wie z. B. das Produktmanagement und die Entwickler, werden vor der Einstellung einer Sicherheitsüberprüfung unterzogen.

Monitoring und Reaktion auf Vorfälle

Extreme Networks verfügt über einen technischen Support, der rund um die Uhr zur Verfügung steht, sowie über zusätzliche Mitarbeiter, die auf Abruf bereitstehen, um auf Vorfälle zu reagieren. Falls Extreme eine Sicherheitsverletzung oder einen anderen schwerwiegenden Sicherheitsvorfall feststellen sollte, eskalieren die Mitarbeiter von Extreme die Situation sofort, untersuchen sie und schaffen nach Bedarf Abhilfe.

Benachrichtigungen bei Sicherheitsverletzungen

Im Falle eines Verstoßes und nach der Feststellung, dass kundenspezifische Daten kompromittiert wurden, benachrichtigt Extreme die betroffenen Kunden entsprechend der CloudIQ Datenschutz-Richtlinie.

Verfügbarkeit

Uptime

Das SLA für ExtremeCloud IQ finden Sie im ExtremeCloud IQ Service Agreement.

Disaster Recovery (DR)

Der DR-Plan von Extreme Cloud IQ umfasst tägliche Backups für alle Daten innerhalb der regionalen Rechenzentren und die Replikation dieser Backups zwischen den geografischen Regionen. Die Backups werden 30 Tage lang aufbewahrt. Alle replizierten Sicherungsdaten werden für alle in den USA ansässigen Rechenzentren innerhalb der USA und für alle anderen Rechenzentren innerhalb Europas aufbewahrt, um die Anforderungen an die Datenhoheit zu schützen.

Verfügbarkeits- und System-Monitoring

Extreme setzt auf unserer Cloud-Infrastruktur ein kontinuierlich arbeitendes, verteiltes System für das Monitoring von Verfügbarkeit und Performance ein. Es überwacht Anomalien im Verhalten und in der Funktionalität der Anwendung und sendet Warnungen an ExtremeCloud IQ Cloud Operations, damit bei Bedarf sofort gehandelt werden kann. Es ist wichtig anzumerken, dass ExtremeCloud IQ eine Plattform zur Netzwerkmanagement und zur Orchestrierung der Konfiguration ist und sich nicht im gleichen Pfad wie die Kundendaten befindet; außerdem hat sein Betrieb keinen Einfluss auf die Zugriffsmöglichkeiten von Endanwendern oder Geräten auf das Netzwerk.

Backup- und Speicherstrategie

Extreme Networks führt täglich Backups für die ExtremeCloud IQ-Umgebung durch.

Die Backups werden dupliziert und dreißig (30) Tage lang aufbewahrt. Eine Master-Kopie der Sicherung wird in der CloudRegion für das RDC gespeichert, die zweite Kopie wird in einer anderen Region gespeichert. ExtremeCloud IQ hält sich an geografische Datenrichtlinien, und alle Backups werden nur innerhalb ihrer geografischen Ursprungsregion repliziert. (d. h. US-Backups werden nur in US-Regionen repliziert, und europäische Backups werden nur in europäische Regionen repliziert).

Die Backups werden sowohl auf lokalen als auch auf Remote-Servern in einem komprimierten und verschlüsselten Format gespeichert und sind für Anwender unzugänglich. Nur authentifizierte Anwender der administrativen Ebene können auf alle Backups zugreifen. Die Wiederherstellung von Kundendaten im Einzelfall ist nicht möglich, da Backups nur zur Wiederherstellung eines gesamten Regional Data Centers (RDC) verwendet werden können.

Die Backups werden mindestens einmal jährlich gemäß den dokumentierten Disaster-Recovery-Testanforderungen von Extreme Networks getestet.

Innerhalb der Anwendung ist ein individuelles Backup der Kundenkonfiguration zulässig. Kunden sind für die Durchführung regelmäßiger Backups ihrer Umgebung selbst verantwortlich, wenn sie davon ausgehen, dass sie einzelne durch administrative Fehler, Unfälle oder böswillige Mitarbeiteraktionen verlorene Objekte wiederherstellen müssen.

Die Sicherung der Kunden VIQ kann von jedem autorisierten Administrator einfach über die ExtremeCloud IQ GUI durchgeführt werden. Informationen dazu finden Sie in der Hilfedokumentation der Anwendung oder über den technischen Support von Extreme Networks (GTAC).

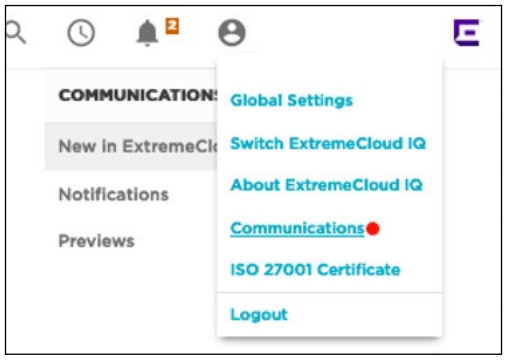
Benachrichtigung und Support

Technischer Support

Der Support für ExtremeCloud IQ ist 24x7x365 über das Support-Portal verfügbar. Hier können Tickets mit GTAC (Global Technical Assistance Center) geöffnet werden, und Sie erhalten Zugang zu einer vollständigen Knowledgebase und Dokumentation.

Kundenbenachrichtigungen

Kunden werden über die Registerkarte „Notifications“ innerhalb von Extreme Cloud IQ über anstehende Releases, Standard-Wartungsarbeiten und andere Bulletins benachrichtigt. Um darauf zuzugreifen, klicken Sie auf die obere rechte Ecke des Bildschirms, wenn Sie eingeloggt sind, und wählen wie unten gezeigt den Link „Communication“.



In seltenen Fällen kann es vorkommen, dass ExtremeCloud IQ Cloud Operations Sie zusätzlich zur Benachrichtigungsseite per E-Mail über dringende oder andere wichtige Wartungsankündigungen benachrichtigt, die ein Handeln im Namen des Kunden erfordern.

Wir empfehlen Ihnen dringend, alle E-Mails von „communication@extremecloudiq.com“ in Ihrer SPAM-Lösung und Ihrem E-Mail-Client zuzulassen, damit Sie keine wichtigen Benachrichtigungen verpassen.

Abgesehen von den oben erwähnten Email-Benachrichtigungen erhalten Sie dreißig (30) Tage im Voraus eine Benachrichtigung über jede Wartung oder Aktualisierung, die ein Eingreifen des Kunden erfordert. Eine letzte Benachrichtigung wird sieben (7) Tage vor Beginn der Aktivität versandt.

Modell der geteilten Verantwortung

Wie bei jeder SaaS-Lösung liegt die Sicherheit Ihrer Daten in der gemeinsamen Verantwortung. Extreme Networks arbeitet Hand in Hand mit Ihnen, denn nur gemeinsam können wir eine sichere Umgebung bereitstellen.

Verantwortung von Extreme Networks

Extreme Networks ist verantwortlich für

- Die Aufrechterhaltung der Betriebsbereitschaft der ExtremeCloud IQ-Plattform, einschließlich
  - Networking und Konnektivität
  - Betriebssysteme, Container und Container-Management-Lösungen (Kubernetes)
  - Speicherung und Aufbewahrung der Daten
  - Disaster-Recovery-Planung, Tests und Backups der Lösung
- Die Aufrechterhaltung des SLAs von ExtremeCloud IQ auf oder über den veröffentlichten SLA-Anforderungen
- Die Sicherstellung rechtzeitiger Sicherheitspatches und Wartung für alle Services und Systeme, aus denen ExtremeCloud IQ besteht
- Die Sicherung aller Daten im Ruhezustand und bei der Übertragung unter Verwendung von Verschlüsselungsprotokollen und -methoden nach Industriestandard sowie Verwaltung aller kryptografischen Kontrollen innerhalb der Lösung
- Den Schutz der Daten mit Architektur und Prozessen zur Erhaltung der Datenbeständigkeit

Verantwortung des Kunden

Der Teilnehmer (Kunde), der ExtremeCloud IQ verwendet, ist verantwortlich für

- Die Erstellung und Implementierung aller verwalteten Gerätekonfigurationen und individuellen Gerätesicherheitsstandards, die in der Kundenumgebung verwendet werden
- Die Sicherstellung, dass die Konfiguration und die Sicherheitspraktiken, die zur Konfiguration und Sicherung der Geräte im Kundennetzwerk verwendet werden, den Best Practices der Branche entsprechen
- Die Aufrechterhaltung der Internetkonnektivität durch korrekte Firewall-Regeln und angemessene Bandbreite und Latenz, um die Konnektivität der verwalteten Geräte mit ExtremeCloud IQ zu gewährleisten
- Die Sicherung von Anwendernamen und Passwörtern und anderen Anmeldeinformationen, die für den Zugriff auf ExtremeCloud IQ verwendet werden, um deren Offenlegung gegenüber nicht autorisierten Personen zu verhindern
- Die Aktualisierung der Firmware angeschlossener Netzwerk-Geräte und die Installation ausgegebener Patches für Sicherheitsrisiken, wie von Extreme Networks empfohlen
- Die Durchführung von Backups ihrer VIQ-Umgebung mit Hilfe von Tools innerhalb der Anwendung, um den Kunden bei der Wiederherstellung nach administrativen Fehlern, Unfällen oder böswilligen Mitarbeiteraktionen zu unterstützen
- Die Nutzung der Lösung in Übereinstimmung mit den ExtremeCloud IQ Cloud Terms of Service
- Die rechtzeitige Beantwortung von GDPR- oder anderen Datenschutzanfragen, die Sie erhalten, und Beantwortung von Anfragen, die Sie an Extreme stellen, in einer angemessenen Weise

In ExtremeCloud IQ verfügbare Daten und PII

Provider	Details zur Sichtbarkeit persönlicher Daten des Endkunden
Infrastruktur-Provider (AWS, Google, Azure)	Cloud-Infrastruktur-Provider sind nicht berechtigt, auf Daten in ExtremeCloud IQ zuzugreifen bzw. diese einzusehen. Der gesamte Zugriff ist auf private Instanzen isoliert, auf die nur über Anlagen von Extreme Networks und durch eine begrenzte Anzahl von Mitarbeitern von Extreme Networks zugegriffen werden kann.
Customer Support Provider (Extreme GTAC)	**Für das GTAC sind keine Daten zugänglich, es sei denn, sie werden vom Kunden-Engineering freigegeben.**
DevOps/Development (Extreme Engineering)	**Zugang zur Liste der Kunden (MSP, Kunden), die ExtremeCloud gekauft haben**
	Gerätespezifische Daten des Endanwenders
	MAC-Adresse
	Gerätehersteller (Apple, Samsung, Intel, etc...)
	Letzte zugewiesene IPv4- und IPv6-Adresse
	Hostname
	Funkattribute und -fähigkeiten
	Standort (WLAN-App, mit der das Gerät verbunden ist)
	„Wo im Netzwerk"-Daten des Endanwenders
	Letzter Zeitpunkt, an dem der Anwender im Netzwerk sichtbar war
	Zuletzt verbundener AP
	Zugewiesenes Netzwerk-VLAN
	Historischer Roaming-Verlauf („Wo waren Sie zum Zeitpunkt X?")
	Zuletzt verbundenes spezifisches Netzwerk/SSID
	„Welcher Netzwerkstandort"-Daten des Endanwenders
	Geografischer Standort, an dem der Anwender zuletzt sichtbar war
	Spezifische „Site", an der der Anwender zuletzt sichtbar war
	Netzwerknutzungsdaten des Endgeräts
	Wireless-Statistiken und zusammenfassende Ereignisse über einen bestimmten Zeitraum
	Fehlerraten über einen bestimmten Zeitraum
	Zuletzt gemeldeter Funkkanal, Band und RSS für das Gerät des Anwenders
	Vom Gerät/Anwender verwendete Anwendungen
	Anwenderspezifische Daten (nicht Captive Portal)
	Bei Verwendung von 802.1x, eingeloggter Anwendername
	Bei Verwendung von PPSK, PPSK- oder E-Mail-Adresse des Anwenders
	E-Mail-Adresse
	Anwenderspezifische Daten (Guest Captive Portal/Social Login)
	Telefonnummer (falls übermittelt und erforderlich, für PPSK-Authentifizierung)
	E-Mail-Adresse (falls übermittelt und erforderlich, für die PPSK Authentifizierung)
	Administratordatum (wird zum Erstellen von Cloud-Administratoren verwendet)
	Vor- und Nachname des Administrators
	E-Mail-Adresse des Administrators
	Stadt, Bundesland, Land des Administrators
	Firmenname
	Branchenzugehörigkeit des Unternehmens (Einzelhandel, Bildungswesen, etc.)
	Telefonnummer des Administrators
Anbieter	**Anbieter haben keinen Zugriff auf die Daten**

Extreme networks

https://de.extremenetworks.com/kontakt/